Strategy Research Project

Biometrics Technology

by

Lieutenant Colonel Rodney E. Garfield
United States Army

U.S. ARMY WAR COLLEGE
Prudens Futuri
Carlisle Barracks, PA

United States Army War College
Class of 2012

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 13-03-2012	**2. REPORT TYPE** Strategy Research Project	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE
Biometrics Technology

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Rodney E. Garfield

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Colonel Robert M. Mundell
Department of Command,
Leadership, &
Management

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In the aftermath of the terror attacks of September 11, 2001, the United States along with the international community finally realized the risk to its sovereignty, peace and way of life. The methodologies, techniques and practical application of biometrics technology, once implemented fully as a deterrent, will safeguard and secure key U.S. infrastructure, networks and platforms as we continue to transform and downsize the Department of Defense (DoD) in the twenty-first century. This strategic research effort examines biometrics technology with an emphasis on the advantages and disadvantages as they apply to the Department of Defense given current fiscal constraints and budgetary concerns. This paper will define and examine several of today's most utilized biometric techniques from their inception to their more recent employment, and concludes by providing recommendations for senior Army leaders to consider as they apply to the employment of biometrics.

15. SUBJECT TERMS
C4I

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UNCLASSIFED	**b. ABSTRACT** UNCLASSIFED	**c. THIS PAGE** UNCLASSIFED	UNLIMITED	28	**19b. TELEPHONE NUMBER** *(include area code)*

USAWC STRATEGY RESEARCH PROJECT

BIOMETRICS TECHNOLOGY

by

Lieutenant Colonel Rodney E. Garfield
United States Army

Colonel Robert M. Mundell
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel Rodney E. Garfield

TITLE: Biometrics Technology

FORMAT: Strategy Research Project

DATE: 13 March 2012 WORD COUNT: 5,619 PAGES: 28

KEY TERMS: C4I

CLASSIFICATION: Unclassified

In the aftermath of the terror attacks of September 11, 2001, the United States along with the international community finally realized the risk to its sovereignty, peace and way of life. The methodologies, techniques and practical application of biometrics technology, once implemented fully as a deterrent, will safeguard and secure key U.S. infrastructure, networks and platforms as we continue to transform and downsize the Department of Defense (DoD) in the twenty-first century. This strategic research effort examines biometrics technology with an emphasis on the advantages and disadvantages as they apply to the Department of Defense given current fiscal constraints and budgetary concerns. This paper will define and examine several of today's most utilized biometric techniques from their inception to their more recent employment, and concludes by providing recommendations for senior Army leaders to consider as they apply to the employment of biometrics.

BIOMETRICS TECHNOLOGY

> "Together we will confront the threat of terrorism. We will take strong precautions aimed at preventing terrorists' attacks and prepare to respond effectively if they come again. We will defend our country; and while we do so we will not sacrifice the freedoms that make our land unique."
>
> —President George W. Bush, October 8, 2001.[1]

Protecting America and the freedom of its citizens was important during the formulation and writing of the U.S. Constitution, during and after the attack on Pearl Harbor, and it remains important in the aftermath of the tragic terrorists' attacks of September 11, 2001. As Americans, we have become so complacent and content that we have begun to take our normal day-to-day freedoms for granted, and why shouldn't we? Most Americans today are not familiar with the events associated with the Japanese attack against Pearl Harbor, and prior to the 9-11 attacks, the nation's citizens would have significantly rejected the idea of waiving their rights to protect civil liberties. Even today the nation is relatively secure, and Americans continue to go about their daily lives as they have in the past. Citizens assume they will be protected by the DoD against both home grown criminals and terrorist organizations. In order to sustain this dynamic, the American public, lawmakers and the U.S. President must be even more determined than the nation's adversaries in order to prepare for and face unforeseen challenges that lie ahead. The U.S. must garner all resources and take a more proactive approach towards safeguarding and protecting its borders, ports, airlines and the homeland. All of this must be accomplished in a resource constrained environment and with a very limited budget. As the largest agency in the U.S. Federal Government, DoD is manned with consummate professionals, is well equipped, and resourced and is the only agency capable of orchestrating and leading the effort to ensure every American's freedoms are protected as outlined in the U.S. Constitution. Biometrics is an integral part of this enduring and daunting requirement.

In today's challenging times of budget constraints and scarce resources, the DoD will find itself in a constant struggle to balance all of its requirements, and to more importantly, maintain or exceed the technological pace of its adversaries. Given the current U.S. fiscal situation, policymakers will look to make drastic cuts across DoD to curtail the debt crisis, remain relevant and maintain the nation's standing as the world's greatest super power. As a result, the DoD must gain efficiencies in its acquisitions processes.

With the appointment of The Honorable Ashton B. Carter to the position of Deputy Secretary of Defense and the acting Under Secretary for Defense for Acquisition, Technology and Logistics (USD(AT&L)), DoD will now be required to take a more direct and a hands-on approach in order to streamline the defense acquisition process while safeguarding and protecting the nation and its citizens. To meet this objective, the current process in place will need to be more efficient and cost effective. In light of a new business model approach designed to help DoD cut cost, commercial off the shelf technology (COTS) should assist the government and private sector. One example of this type of technology is biometrics. Biometrics, is maturing at a rapid pace, appears to be one of the most promising and developed fields of study today, and is critical in the protection of the homeland.

Today the DoD no longer has a competitive edge in the commercial sector, and as the entire federal government budget continues to decrease, DoD will have to "look for new and innovative ways to maximize their spending power in order to effectively" use each and every dollar within current constraints. COTS provides this potential. In the past, weapon's development and system requirements were developed in concert with new products and new technology. Conversely, the commercial markets of today drive product and technology development.[2] This circumstance leads to a very important question, should DoD continue to rely heavily on commercial hardware and software?

During the last decade, DoD began to extensively leverage more commercial hardware and software in an effort to get equipment into the hands of warfighters downrange. The warfighters stressed the current acquisition process so badly that the cause and effects produced an enormous amount of operational need statements (ONS) and joint urgent operational need statements (JUONS) to "bridge the cap" in an effort to shorten the time between requirements generation and equipment delivery. Overseas Contingency Operations (OCO) was the primary funding account code designed to fund the majority of these projects supporting both conflicts in Afghanistan and Iraq. The "just in time" fielding of the Mine-Resistant, Ambush-Protected (MRAP) vehicle designed to protect service members in the United States Central Command (USCENTCOM) area of operations against improvised explosive devices (IEDs) is just one example of DoD efforts to leverage commercial hardware. As the DoD begins to draw down forces in Afghanistan, and OCO funds are terminated, these types of sourcing techniques cannot be sustained. However, COTS still has a significant role to play as it applies to acquisition practices in support of operational requirements.

What is Biometrics?

"The term "biometrics" is derived from the Greek words "bio" (life) and "metrics" (to measure)."[3] Simply stated, biometrics is scientific technology that uses several different methods and techniques to identify a human being's individual characteristics. To the average citizen, biometrics is still somewhat of a mystery and is probably thought of as something associated with a "Star Wars" movie. However, many scientist and security professionals understand the importance of biometrics and the potential it has to revolutionize the way criminals and terrorists are prosecuted. In a world plagued with criminal and terrorist activity, advancements in technology have become critically important, and the ability to quickly identify a person is essential. Biometrics provides this capability.

The need to identify a person is not a new phenomenon, and primitive forms of biometrics have been used in some form or another since the beginning of civilization. For example, early forms of biometrics were used in "Babylon in 500 B.C. by recording fingerprints in clay tablets to record business transactions."[4] Another early form of biometrics was simply using the human face as a means of identification. "Easily recognized, humans have used this distinguishing feature to identify both known and unknown individuals. However, as population centers grew, the task of identifying individuals became more complex and challenging."[5] "The true essence of biometric identification began to surface in the latter half of the twentieth-century with the development of the mainframe computer."[6] There are several forms of biometrics technology that are of interest to the U.S. Federal Government, and two of the most common forms of biometrics are physical and behavioral.

Biometrics Solutions (Types-Physical & Behavior)

One of the most well-known forms of physical biometrics is fingerprinting, which stems from research conducted in the late 19th century by Alphonse Bertillon, a French criminologist who developed the first known means of anthropometry, which literally means measuring humans.[7] Bertillon strongly believed that each individual was created differently and possessed unique traits and characteristics. According to his logic, nature never repeats itself and dissimilarities are captured in the characteristics of the body. Bertillon devised a method of identifying human beings by using a description of bodily characteristics to include, "eye color, hair color, height, weight, and fingerprints."[8] This system was later named Beritillonage, and was intended to minimize risks and problems associated with the identification of criminals based solely on rudimentary information such as a person's name and residence.[9]

Although early scientific discovery in the field was promising and several countries employed the system to include Russia, England, the United States, Belgium, and Switzerland, there were many flaws in the system that influenced its reliability and accuracy, and as a result, the system's utilization and effectiveness declined dramatically giving birth to fingerprinting.[10]

The basic principle behind fingerprint biometrics technology is that there are no two hands, fingers or toes alike because they don't have the same dermal ridge characteristics. "A fingerprint is made primarily of ridges and valleys on the surface of the finger."[11] To correctly determine an individual's fingerprint, the patterns, furrows and minutiae points must be measured, all must match and all must be positively identified. All humans, although different and unique in their own way, have "five basic fingerprint patterns: arch, tented arch, left loop, right loop and whorl."[12]

While the usefulness and effectiveness of fingerprinting biometrics as a deterrent to criminal and terrorist activity is apparent, there are still issues with employing this form of physical biometrics. For example, the fingertip is a very small area to measure, and the area is susceptible to infection, cuts, dirt and other forms of abuse due to wear and tear. Additionally, some doctors or medical professionals use strong chemicals before, during and after surgery to sanitize their hands and as a result, these techniques limit the use of fingerprinting.[13] However, the application of fingerprinting technology is being used more extensively in today's common wireless devices such as laptop computers, IPads and cellular phones. One marked advantage these devices have is that they are inexpensive and power requirements are minimal and relatively low in comparison to other devices.

In the latter part of the twentieth century, law enforcement agencies at every level of the government began to leverage fingerprinting technology in order to conduct screening and background checks.[14] Currently, fingerprinting is used around the world in countries like the United Kingdom (UK), the U.S. and Belgium in a number of ways at the local, state and national level in both commercial and government sectors. It is also used extensively by law enforcement agencies at every level of the U.S. government to include the U.S. military particularly during recent operations specific to the War on Terrorism. In the U.S. today, it is easy to find several hundred commercial vendors employing fingerprinting technology as a deterrent to criminal activity. These examples range from gaining access to a basic laptop computer installed with a Personal Computer Memory Card (PCMCIA), to gaining access to your room in 4 and 5 star hotels. Even though the technology has its disadvantages, such as documented cases where fingerprinting biometrics was used to wrongly convict an innocent person. There are more cases today where the technology was used and proven reliable to justifiably acquit an innocent person, and the benefits clearly outweigh the negative aspects associated with the use of fingerprinting.

Another form of physical biometrics is facial recognition. “Facial recognition unlike other systems identifies individuals by analyzing the unique patterns and contours of an individual’s facial features.”[15] This form of biometrics is believed to have originated back to the early 1960s. “One of the leading pioneers in facial recognition biometrics was Woodrow W. Bledsoe who developed a system to analyze the eyes, ears, nose and mouth by using a photograph.”[16] The system utilized the contrast of facial features to determine useable points, and overlaid the points and features to a common reference point on the face.[17] In layman’s terms, this biometrics technique and method verifies an individual by using a video image, and simply compares and contrasts the feature of the face with an existing database by looking for a positive identified match.

There are several advantages associated with Facial recognition. It is highly reliable, used extensively in security systems, and is often times compared to fingerprinting or eye iris recognition systems.[18] Unlike other current technologies in existence today, this method can acquire the subject in question without the subject ever knowing. As an example, during a professional football game in Florida in 2001, facial recognition technology software was used to positively identify 19 potential criminals with minor police records.[19] The state of Pennsylvania’s has used the same technology to solve a number of cases that have been in existence for years.[20]

While facial biometrics has proven reliable and is worth the effort to employ, there are some critics completely opposed to the use of facial recognition biometrics usage in both the open market and private sectors primarily because they feel it violates a person’s civil liberties and privacy rights. For the most part, their concerns are centered on the employment of surveillance and video technologies at the local, state and federal levels. Critics argue that regardless of the level of government, current threats to the nation do not warrant such drastic measures such as videotaping citizens without their explicit knowledge, based on the government possessing the capability and ability to monitor the activities and locations of all Americans.[21] In the wake of 9/11 and with the increased need to secure the U.S. homeland and critical infrastructure, the advantages of implementing more stringent biometric technologies such as facial recognition clearly exceed that of the naysayers.

The hand geometric recognition physical biometric system is similar to fingerprinting; however, it is based solely on hand measurements, to include the shape, size, length and finger width.[22] Relatively speaking, the system is one of the best methods ever developed and has been used in a myriad of venues throughout the world. Several corporations, military units and law enforcement agencies currently use hand geometry to protect merchandise and safeguard their employees. One of the most well-known and documented cases where hand geometry was effectively used was during the 1996 Olympic Games in Atlanta, GA. During this event, the system was used as an inexpensive method designed to safeguard people in attendance. The system was employed much earlier than projected due to the massive number of people expected to attend the Olympic Games. During the Olympics, it was estimated that over 65,000 people were entered into the database and in excess of 1 million transactions were processed.[23]

From a historical perspective, the two leading methods of eye biometric identification are the iris scan and retina scan, both of which have excellent success rates for positive identification. Scientific studies have shown that iris recognition is the most accurate form of physical biometric identification in use today. Several American entities and organizations to include the DoD have begun to experiment in this critical field of technology to advance security both home and abroad. One company, Iridian Technologies, is believed to be the front runner in the field of science and technology and has developed a system that monitors, tracks and reads three times as many characters as other technologies. Today, the technology is used in airports throughout the U.S. and around the world. With this ability, the accuracy rate is 50% better than fingerprinting as it applies to positively identifying criminal activity because a person's iris remains constant from the age of one. As a result, if a child were to have their iris scanned it would be the same with no deviations and remain valid for a lifetime.[24]

Iris recognition is less intrusive than retina scanning and this physical biometric capability has an array of other advantages. To begin with, COTS iris scanning systems are very easy to use, and simply require a camera and a means of recording the photograph of the retina. Individuals being recorded only have to stand approximately three to ten inches from the camera. The system automatically scans the iris with an invisible infra-red light that captures explicit details of the eyes not normally visible to the naked eye. "The system aggressively interrogates and examines the eyes in a manner similar to that of other biometric identification methods through a detailed analysis and digitized image, and compares the image against a known reference for verification."[25] Interest in the advancement of this technology spans across both academia and industry and has grown significantly over the last decade. To date, some “50 million persons worldwide have been enrolled in iris recognition systems and DoD is key player in this endeavor.”[26]

Retina scanning technology like iris scanning also uses unique eye patterns specific to an individual that have been obtained over a period of a person’s life to confirm an individual’ identity. Retina scanning is the older of the two technologies and is by far more intrusive than the iris scanning technique. While many organizations have reported complete satisfaction in the accuracy of the system, others have concerns with the system because of the discomfort it causes during the scanning procedure. “The system’s basic functions require an individual to look into a retinal and focus on a visible target until the scan is completed.”[27] As a result, public and private sector acceptance of the system is lacking. However, the system has gained more and more acceptance as the federal government continues to invest more research and development funding toward its advancement in support of operational military requirements. Currently, “retina scan security systems are used almost exclusively in high end security facilities such as nuclear power plants, and advanced research installations just to name a few.”[28]

One of the newest forms of physical biometric technologies to hit the market in recent years is the hand vascular pattern or vein pattern technology. This method uses the genetic structure and makeup of the subcutaneous vascular network that varies from person to person on the back of the hand to confirm an individual’s identification. The theory and science behind this recent discovery has proven so accurate that it can delineate the characteristics between identical twins.[29] Although it is a nascent technology, it is highly sought after, and has proven fairly successful and reliable in certain markets in Southeast Asia in particular.[30]

The first prototype, the BK 100, surfaced in 1997, and was strictly limited in its original use to physical access control. However, today the system is used extensively in deterring criminal activity in the finance and banking industry, travel and transportation, hospitals, construction sites and schools. Unlike other identification technologies in existence today, the hand vascular pattern has not met traditional industry evaluation criteria, and has not been completely validated through a formal process by government officials.[31]

Just about every cop show on television today highlights the advantages of leveraging DNA testing, another form of physical biometrics, to solve crimes. DNA testing and usage has revolutionized the way law enforcement agencies accurately identify criminals more so today than it did in previous years. DNA evidence has been used to support criminal investigations since the early 1980s. DNA testing has proven to be fairly accurate, mainly because the chance of 2 people having the same DNA makeup is believed to be less than one in a hundred billion.[32] Technology associated with DNA testing has grown in retrospect, and is more advanced in comparison to previous methods employed. Although this biometrics technique has proven successful, the technology is faced with legal challenges posed by civil liberty organizations, and collecting DNA samples is expensive and often times requires long lead times to conduct testing. Even given these disadvantages, the federal government and the DoD should make every attempt to advance the current technology in order to prevent terrorist organizations from doing harm within the U.S. and minimize criminal activity.

Another form of physical biometric technology is voice recognition. DoD uses voice recognition software extensively on its computer networks and telephone distribution systems in comparison to the private industry. With the global expansion of the telephone industry, especially wireless and Voice over IP (VoIP) networks in particular, voice biometrics is rapidly becoming one of the leading technological advances because of its reliability coupled with the fact that there are no overhead or additional costs required to employ the system. Based on this fact alone, voice biometrics has a clear and distinct advantage over other biometric technologies.[33] The technology has matured over the last several years and its application is widely used in computer networks such as screen savers and large telephone systems in the commercial and governmental sector.

Signature verification is a form of behavioral biometrics and is considered one of the oldest forms of identity verification. Even though the act of writing a signature is physical in nature, signature verification falls into the category of behavioral biometrics because a person's emotional and physical state severely determines and impacts the outcome of a signature when it is written.[34] The acceptance of signature verification has been overwhelming and its use in global markets today is widespread. This identification system has outpaced all other systems currently in use today, thanks largely in part to the consumer's need for real-time data at their fingertips and the need to have immediate access to the internet while mobile. While the system remains very popular, there are disadvantages to the present system that can be summed up in two categories. First there is the casual imposter. This circumstance occurs when there is little to no known information readily available pertaining to an individual whose identity is being compromised. The second category is the real impostor, where adequate to substantial information is known about the victim whose signature is being compromised.[35]

Keystroke Dynamics is another form of behavioral biometrics that came to fruition with the invention of the mainframe computer. Keystroke dynamics refers to sounds generated when typing on a computer's keyboard and is based on the unique and distinct rhythms that occur when a specific individual uses a computer keyboard. Although there is adequate data to support this theory and as exciting as this may sound, it is by no means worthy to positively identify two distinct individuals from one another. Thus, it is one of the least utilized systems in the commercial and government markets and is completely software based unlike previously mentioned biometrics technologies.[36]

The final biometrics technology this paper will address is the smart card. DoD implemented the Common Access Card (CAC) for active and reserve military personnel, DoD civilian and key contractor personnel. The initiative was designed to enable users to quickly and securely gain access to federal military installations and buildings, and more importantly, to access DoD government computer network systems using embedded encryption. The earliest version of the CAC was the smart card or automated chip card that was developed in the late 1960s in Europe by a German engineer named Helmut Grottup. [37] The smart card quickly received broad acceptance in Europe over the past three decades before being commercialization in the U.S. The smart card's popularity grew because of its size and storage capacity. It is no larger than a small wallet containing an integrated circuit to provide security.[38] The primary advantage associated with smart cards in comparison to other forms of biometrics technology is that they are small and inexpensive to manufacture. In a resource constrained environment, the DoD could leverage smart cards in so many ways to defer cost to service members and civilian employees. In addition, smart cards have become highly sought after because of their growing use in the global market. DoD quickly began to expand the use of the CAC because of its security features, notoriety and its reliability as a form of electronic identification.[39]

The Importance and Advantages of Biometrics

There are several historical examples that highlight the need as well as the concern for increased security. During World War I, Congress passed the Espionage Act due to concerns over communist and espionage activities in the country. The Act primarily dealt with espionage, but it also addressed freedom of speech in an effort to protect military secrets.[40] This historical example is an important aspect and security consideration that provides the basic framework for all future discussions and conflicts that lie ahead. It also provides the rationale for enhanced and increased security in times of war, and has become more of a concern in the U.S. with an aggressive, adaptive and determined adversary who did the unthinkable to the world's premier super power on September 11, 2001.

One major advantage of implementing biometrics today is the ease of integrating different systems into an already established architecture. Earlier systems generally lacked the ability to efficiently integrate legacy systems into existing architectures due to numerous interoperability and configuration challenges. Moreover, these legacy systems did not codify business processes in an effort to negate the challenges with the integration of older systems. The "system of systems" business model approach can resolve all future interoperability issues. One way that the DoD can implement this approach is by fusing hand and fingerprinting technologies into one database. As a result, stored information will contain all unique characteristics associated with an individual's hand and fingers, making it easier and faster to indentify criminals. What used to take days and weeks with regards to collecting and shipping samples off to a laboratory for testing, will now only take hours by combining the two systems together. Normally, this has not been the case as there was one system primarily set aside for hand geometry and a totally different system for fingerprint identification. Combining the two systems will also lower procurement and manufacturing cost, making biometrics more appealing and affordable for DoD to implement.

Another advantage for implementing biometrics is the ability to safeguard and protect an individual's civil liberty and privacy rights. Privacy concerns emerge when individuals do not consent to their personal information being used by third parties regardless for what purpose. The concern comes into play for example when a cellular telephone company sells your personal information; where you live, your complete name and e-mail address to another consumer, this in itself completely violates your right to privacy. However, this is not the case with the modern biometrics used in defense of the homeland and in support of the Global War on Terrorism. When fingerprinting and other physical types biometrics are strictly used to clearly identify a person in support of law enforcement agencies and DoD to swiftly prosecute criminals and terrorists, they do not in any way, shape or fashion violate any constitutional laws. DoD through discovery learning primarily as a result of being at war the last ten years, will only employ biometrics when there is sufficient evidence beyond a reasonable doubt to convict someone accused of committing a crime.

The attacks of September 11 reminded the U.S. and the world that none of us are truly safe and completely secure from criminal and terrorists acts. However, instituting some of the obtrusive techniques designed to gather critical information pertaining to suspected acts of terror violate individual freedoms and do not guarantee the nation's safety. In light of this fact, DoD must allocate resources and add biometrics to the Cyber Domain in order to safeguard systems inherent in both the services and the combatant commands. Implementing this plan of action and methodology does not require any additional force structure to an already "out of balance" joint force.

In the aftermath of 9/11, inspired by the insistence of the American public, the U.S. legislative branch finally approved legislation exclusively to use biometric technology as a system of identification. This was enabled by enacting "The USA PATRIOT Act of 2001 and the Enhanced Boarder Security and Visa Entry Reform Act of 2002." These legislative actions highlight the important role biometrics technology plays in the war on terror.[41] The biometric techniques addressed earlier in this paper provide the government and private sector the security necessary to ensure protection both at home and abroad. In light of the recent vulnerabilities to the banking institutions, federal government and social security department computer systems must be protected at all costs.

Leveraging biometrics at a reasonable cost in a time of war and during the U.S. economic crisis is clearly important in comparison to other security means currently in existence, and conditions are set for the biometrics industry to capitalize on a fluid market that is in urgent need of improving its security posture. In the U.S. alone, the biometrics market is estimated to cost in excess of $4 billion, and constitutes roughly an 80% growth from previous years.[42] As a point of reference, the current U.S. deficit is $15 trillion, and the aforementioned $4 billion dollars is a drop in the bucket.

Leaders in the biometric industry, International Biometrics Industry Association established in 1998 and the Biometric Consortium in 1995, continually debated with the public pertaining to reliability and performance as they emphasize security and the applicability of biometric technology as a deterrent to criminal activity. Despite the many pessimists and negative rhetoric, "the United Arab Emirates (UAE) effectively employed the Iris Deportation Tracking System (IDTS) in 2001 to stop the re-entry of individuals that had been deported from the country." [43] The initial design used by the UAE was completely user-friendly and immediately proved its worth. The system proved very accurate and the UAE Government was thoroughly impressed with its daily processing speed. The system's central database was able to cross reference up to 12,000 searches per day, preventing illegal aliens from entering the country.[44] In addition, the system is completely comprised of several COTS components that can be purchased at a reasonable cost from commercial venders. One challenge the biometric industry has taken on and determined as critical is developing systems that are easily interoperable with current systems. Even with this issue, the advantages still outweigh the disadvantages.

Recommendations

"We also must never forget the most vivid events of recent history. On September the 11th, 2001, America felt its vulnerability – even to threats that gather on the other side of the earth. We resolved then, and we are resolved today, to confront every threat, from any source, that could bring sudden terror and suffering to America."[45] DoD can no longer sit on the sidelines and allow our adversaries to exploit our weaknesses. As the largest agency within the federal government, it has the resources in both personnel and funding. As long as we remain at war, DoD will remain focused on securing the homeland and protecting our citizens.

Currently, the Army Chief Information Officer (CIO)/G6 is the executive agent for the Department of Defense Biometrics Management Office (BMO), responsible for the conduct and execution of implementing biometrics standards, policy and procedures for DoD., and is also responsible for communicating and executing the President's guidance pertaining to what type of personal identifiable information (PII) can and shall be collected from U.S. citizens and foreign nationals. Finally, the BMO has the inherit responsibility to train DoD personnel tasked to collect and store personal information on its employees.

While the BMO is organized, structured, equipped, trained and resourced to combat the current security fight, it is by no means capable of addressing requirements associated with homeland security. As a result, assigning a BMO to both the Department of Homeland Security (DHS) and United States Cyber Command (USCYBERCOM), a sub-unified command under United States Strategic Command (USSTRATCOM), will provide the appropriate level of leadership to effectively affect change at the macro level. This additional force structure and emphasis will provide greater support for the nine Geographic Combatant Commands. In addition to the Army G6, these two additional BMOs will work in concert to formulate strategic policy in the defense of the U.S. against terrorist attacks on the homeland and its adversaries, and will also have the responsibility to work directly with other agencies at the local, state and federal levels, private sector and the National Institute of Standards and Technology to develop the future biometrics standards. This change would entail a larger staff and more funding to ensure the aforementioned is set in motion on a path to success for the future of biometrics.

Another challenge that the DoD faces is with "integrating biometrics into a single stand alone system" that is able to record and store data. In seeking to overcome this challenge, DoD should mirror the efforts of the Federal Bureau of Investigation (FBI). The FBI owns and operates its own system and based on its success, many nations' equivalent agencies have sought to mirror it. "The Integrated Automated Fingerprint Identification System (IAFIS) is said to be the largest biometric database in the world, processing over 50,000 daily searches."[46] The system's massive database allows for each CONUS and OCONUS field office to tie into the existing infrastructure on a daily basis.

Conclusion

It is incumbent upon all Americans; more importantly, the Federal Government to take the necessary measures to protect the freedoms of all U.S. citizens. The preamble to the U.S. constitution as drafted by our Founding Fathers highlights the importance of protecting individual freedoms: "We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the commons defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America."[47]

Understanding the essence of the preamble to the constitution coupled with the fact that the United States has been plagued over the last decade with criminal and terrorist activities, now is the time for the DoD to take a more direct approach to protect, safeguard and secure the nation's borders, infrastructure and citizens. The security that biometrics technology provides today is an integral factor in the defense of the U.S. and has proven worthy in both the federal government and commercial sector. As an example, DHS Transportation Security Administration (TSA) improved its policies and security screening procedures for all travelers and today the airlines are more secure than any other time in our nation's history due largely in part to the implementation and use of biometrics.

Although there are still areas for improvements, especially in developing systems that are not stove piped and can easily be integrated with other legacy systems, biometrics technologies are protecting civilians and U.S. service members. Based on these accomplishments, DoD must lead this endeavor and muster the appropriate resources to implement biometrics technology throughout the federal government, by address the challenges that remain with regards to implementing biometrics across the force while simultaneously addressing the issues associated with violating the privacy rights of individuals.

Endnotes

[1] George W. Bush, *Executive Order Establishing the Office of Homeland Security and the Homeland Security Council* (Washington, DC: The White House, October 8, 2001).

[2] Arvid G. Larson, Charles K. Banning, and John F. Leonard, *An Open Systems Approach to Supportability*, (Fairfax, VA: WALCOFF Technologies, June 2002), 1.

[3] Ibid.

[4] National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Biometrics History*, (Washington, DC: National Science and Technology Council, August 7, 2006), 1.

[5] Ibid.

[6] Ibid., 2.

[7] Ibid, 7

[8] ibid, 6

[9] Ibid, 31.

[10] Ibid., 33.

[11] Biometric News Portal, http://www.biometricnewsportal.com/fingerprint_biometrics.asp (accessed December 17, 2011).

[12] Biometric News Portal, http://www.biometricnewsportal.com/fingerprint_biometrics.asp (accessed December 17, 2011).

[13] Ibid.

[14] Ibid.

[15] Lim Doug-hum, "Biometrics as a new technology-Identifying oneself by using unique human characteristics," *The Argus, Theory and Critique,* 1 June 1999 [journal on-line], quoted in Eloy Campos, *Consolidating Our Country's Biometric Resources and The Possible Implications*, Strategy Research Paper (Carlisle Barracks, PA: U.S. Army War College, March 15, 2008), 5.

[16] National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Biometrics History*, (Washington, DC: National Science and Technology Council, August 7, 2006), 8.

[17] Ibid.

[18] Facial Recognition System, http://en.wikipedia.org/wiki/Facial_recognition_system (accessed January 3, 2012).

[19] Ibid

[20] Ibid., 3.

[21] Ibid., 5.

[22] Anil K. Jain, Patrick Flynn, and Arun A. Ross, *Handbook of Biometrics* (New York, NY: Springer, 2008), 16.

[23] National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Biometrics History*, (Washington, DC: National Science and Technology Council, August 7, 2006), 16.

[24] Julian Ashbourn, “Biometric white Paper,” 1999, available from http://homepage.ntlworld.com/avanti/whitepaper.htm, internet, accessed 15 August 2003, quoted in Ray A. Graham. Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, May 3, 2004), 10.

[25] Electronic Frontier Foundation, *Biometrics: Who’s Watching*, September 14, 2003, https://www.eff.org/wp/biometrics-whos-watching-you (accessed January 5, 2012).

[26] Anil K. Jain, Patrick Flynn, and Arun A. Ross, *Handbook of Biometrics,* (New York, NY: Springer, 2008), 71.

[27] Electronic Frontier Foundation, *Biometrics: Who’s Watching*, September 14, 2003, https://www.eff.org/wp/biometrics-whos-watching-you (accessed January 5, 2012).

[28] National Center for State Courts, “Individual Biometrics, “2002, available from http://ctl.ncsc.dni.us/biometrics/BMRetinal.html; Internet; accessed 25 January 2008, quoted in Eloy Campos, *Consolidating Our Country’s Biometric Resources and The Possible Implications*, Strategy Research Paper (Carlisle Barracks, PA: U.S. Army War College, March 15, 2008), 5.

[29] Anil K. Jain, Patrick Flynn, and Arun A. Ross, *Handbook of Biometrics,* (New York, NY: Springer, 2008), 253.

[30] Ibid, 267

[31] Ibid., 267.

[32] Biometric News Portal, http://www.biometricnewsportal.com/fingerprint_biometrics.asp (accessed December 17, 2011).

[33] Anil K. Jain, Patrick Flynn, and Arun A. Ross, *Handbook of Biometrics,* (New York, NY: Springer, 2008), 151.

[34] Lim Doug-hum, “Biometrics as a new technology-Identifying oneself by using unique human characteristics,” *The Argus, Theory and Critique,* 1 June 1999 [journal on-line], quoted in Eloy Campos, *Consolidating Our Country’s Biometric Resources and The Possible Implications*, Strategy Research Paper (Carlisle Barracks, PA: U.S. Army War College, March 15, 2008), 5.

[35] Anil K. Jain, Patrick Flynn, and Arun A. Ross, *Handbook of Biometrics*, (New York, NY: Springer, 2008), 189.

[36] Electronic Frontier Foundation, *Biometrics: Who’s Watching*, September 14, 2003, https://www.eff.org/wp/biometrics-whos-watching-you (accessed January 5, 2012).

[37] Smart Card, http://en.wikipedia.org/wiki/Smart_card (accessed January 10, 2012).

[38] Ibid

[39] Small Card Alliance, *Smart Card and Biometrics: A Smart Card alliance Physical Access Council White Paper*

[40] Lisa S. Nelson, *America Identified: Biometric Technology and Society*, (Cambridge, MA: MIT, 2011), 61.

[41] Lisa S. Nelson, *America Identified: Biometric Technology and Society*, (Cambridge, MA: MIT, 2011), 66.

[42] Ibid., 68.

[43] Anil K. Jain, Patrick Flynn, and Arun A. Ross, *Handbook of Biometrics*, (New York, NY: Springer, 2008), 468.

[44] Ibid.

[45] Post-9/11, http://en.wikipedia.org/wiki/Post-9/11 (accessed January 15, 2012).

[46] Eloy Campos, *Consolidating Our Country's Biometric Resources and The Possible Implications*, Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, March 15, 2008), 10.

[47] U.S. Constitution, Preamble. http://www.constitution.org/constit_.htm